

UNITED STATES DISTRICT COURT

AUG - 7 2019

for the
Northern District of Texas

CLERK U.S. DISTRICT COURT

By: _____
Deputy

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

3 hard drives including a Western Digital 500 GB hard
drive, as further described in Attachment A, located at
FBI Office in Dallas.

Case No. 4:19-MJ-629
FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
3 hard drives including a Western Digital 500 GB hard drive, located at FBI Office in Dallas, as further described in Attachment A.

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

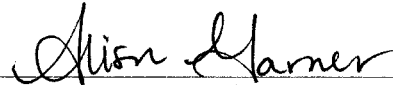
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2252 and 2252A	Possession, Receipt of Child Pornography
18 U.S.C. § 2251	Production of Child Pornography

The application is based on these facts:

See attached Affidavit of FBI Special Agent Alison Garner.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Alison Garner, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/7/19

City and state: Fort Worth, Texas



Judge's signature

Jeffrey L. Cureton, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Alison Garner, a Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the FBI since May 2018. I am currently assigned to the FBI's Child Exploitation Task Force in the Dallas Division. As a FBI Special Agent, I am authorized to investigate violations relating to child exploitation and child pornography, including the production, transportation, receipt, distribution, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have gained experience in conducting these investigations through training and through everyday work, including executing search warrants and interviewing individuals who sexually exploit minors and who possess and trade child pornography. I have also received training relating to the Innocent Images National Initiative, which includes training in the investigation and enforcement of federal child pornography laws in which computers and other digital media are used as a means for receiving, transmitting, and storing child pornography. In addition, I have received specialized training in the investigation and enforcement of federal child pornography laws, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media.

2. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A, Production, Possession and Receipt of Child Pornography.

3. This affidavit is submitted in support of an application for a warrant to search three hard drives (the SUBJECT DEVICES) as further described and depicted in Attachment A, which is incorporated herein by reference. The SUBJECT DEVICES are currently in the possession of law enforcement in the Northern District of Texas.

4. The information contained in this affidavit is based on my personal knowledge and experience, my own investigation, and information provided by other law enforcement officers and/or agents, and by Special Agent Christopher W. Thompson. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause of evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A are located within the SUBJECT DEVICES.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

5. On August 5, 2019, SA Thompson spoke with C.S., a technical employee at 24 Hour Data located at 811 E. Plano Parkway, Suite 124, Plano, Texas. C.S. stated that he is working a job in which a customer requested that 24 Hour Data recover data off of a non-functioning hard drive. That customer is a business named "Nerds to Go," located at 3115 S. Cooper Street, Arlington, Texas.

C.S. stated that after he repaired the drive, a standard quality assurance and data validation check was conducted to ensure that data was indeed recovered. C.S. stated that he observed thousands of files depicting the sexual exploitation of children, including some which appeared to depict a stocky black male with a square beard matching the description of the hard drive's owner, **Tyrone Alexander Taylor**.

6. On August 6, 2019, SA Thompson spoke with T.S., owner of the business Nerds To Go. T.S. stated that **Tyrone Taylor** had brought the hard drive to Nerds to Go on June 22, 2019 for repairs after finding the company on Homeadvisor.com. **Taylor** told T.S. that his daughter had knocked his laptop off of the sofa and the computer could no longer boot from the hard drive. He requested that Nerds To Go repair the drive and recover files, primarily documents and pictures. T.S. advised **Taylor** that Nerds To Go was not equipped to conduct that type of hard drive repair but that they could refer it to a third party company. **Taylor** decided not to pursue that offer and took the drive. On July 11, 2019, **Taylor** changed his mind and agreed to have a third party company evaluate the drive for repairs, and he brought the drive back to Nerds To Go. Nerds to Go then sent the hard drive to 24 Hour Data on July 12, 2019 for evaluation of repair.

7. 24 Hour Data conducted a preliminary examination and determined that the drive could be repaired. They provided a price quote to T.S., who passed the quote on to **Taylor**. **Taylor** said the price was too high and wanted a second price estimate. The drive was then returned to Nerds To Go on July 17, 2019, and was later sent to Secure Data Recovery Services.

Secure Data had the drive for approximately ten days and completed a second evaluation. Neither evaluation actually recovered data; the evaluations were preliminary estimates of repair. After considering both estimates, **Taylor** agreed to have the drive recovered by 24 Hour Data and paid Nerds To Go \$1,385.00 for the services between July 29, 2019 and August 3, 2019. On July 30, 2019, Nerds To Go provided the hard drive to 24 Hour Data for drive repair and data recovery. On the Nerds To Go invoice, the customer is listed as **Tyrone Taylor** at address [redacted] Briaroaks Drive, Fort Worth, Texas 76140.

8. During this time, **Taylor** also requested that his laptop be configured to be operational again. He brought a second hard drive to T.S. (Nerds To Go) who replaced it in the laptop. T.S. installed Microsoft Windows and Microsoft Office on the laptop and returned it to **Taylor** on July 24, 2019, in an operational state.

9. In conversations with T.S., **Taylor** stated that he was in the military and some documents he needed from his service were on the hard drive. **Taylor** said he is a disabled veteran suffering from PTSD for which he receives regular treatment. **Taylor** further stated that he had planned to visit Costa Rica on Saturday, August 3, 2019, for a one week family reunion but changed his mind because this would have his family returning just prior to his daughter's start of school.

10. On August 6, 2019, SA Thompson met C.S. at his place of business, 24 Hour Data. C.S. provided internal tracking documentation and the legal terms and conditions to which Nerds To Go agreed during the negotiation.

Part of the recovery process consists of data validation of recovery so a client's request is properly processed and billed. Part of this validation includes review of specifically requested file recoveries; in this case, **Taylor** requested recovery of documents and pictures.

11. C.S. replaced a hard drive head on **Taylor's** drive at which time the drive was partially readable, although some bad hard drive sectors were still present. C.S. conducted a forensic acquisition of **Taylor's** hard drive, which was placed on a **Western Digital 1 TB hard drive**, further described in Attachment A. C.S. then made a working logical copy of specific folders recovered from the drive, including the "Users" folder, to be used to validate proper data recovery. This working copy was placed on a **Toshiba external 1 TB hard drive**, further described in Attachment A.

12. C.S. stated that during his data recovery validation process, he successfully recovered the "Users" folder of the hard drive. For validation, he reviewed media files. Specifically, on a user Desktop folder, was a series of subfolders, each of which was labeled and contained both images and videos. C.S. observed thousands of files which appeared to depict the sexual exploitation of children, many of which appeared to be homemade. Some of the files depicted an adult Caucasian woman performing oral sex on the penis of a prepubescent boy in a folder labeled "Shannon." Others showed a Hispanic woman performing oral sex on the vagina of a prepubescent female. In other folders, a person matching the description of **Tyrone Taylor** is seen with each of these women and the children. In another image file, a Hispanic woman is seen getting a lower back tattoo which reads "Tyrone Alexander Taylor."

13. C.S. showed SA Thompson one image file named 20170109_180008.jpg. This file depicts an adult black male wearing a white sleeveless undershirt lying on a bed with his pants down. A girl approximately 11 years of age wearing an orange shirt is seen holding a cell phone and placing her tongue on the erect penis of the adult male. The adult male is looking at the camera and smiling.

14. SA Thompson obtained Texas Department of Motor Vehicle records for **Tyrone Alexander Taylor**. These records indicate a date of birth of [redacted] 1977 and Texas driver's license number of [redacted]443. SA Thompson reviewed the driver's license image, and it matches the adult black male depicted in file 20170109_180008.jpg.

15. According to C.S., the same adult black male is seen in a series of images and videos with the woman depicted in the "Shannon" folder. In this series of files, the woman and the man are with a twelve-year old boy, and all of them are having sex with each other.

16. C.S. recovered documents in addition to the media files. He identified one document, which was an image of a driver's license for **Tyrone Taylor Alexander**. The birthdate and license number provided by C.S. match the driver's license SA Thompson obtained from the Department of Public Safety. C.S. also stated the image on the driver's license appeared to be the same adult black male in the pornographic files he recovered.

17. C.S. also recovered a Department of Veteran's Affairs document with the name of "Shannon Nichols" in the title. SA Thompson reviewed Accurint records for **Tyrone Alexander Taylor** and observed that he is associated with "Shannon Nichols" at

address [redacted] Belzise Terrace, Fort Worth, Texas. SA Thompson then obtained Texas Department of Motor Vehicle records for Shannon Nichols at that address. These records indicate a date of birth of [redacted] 1979 and the driver's license image matches the woman depicted in the media files in the "Shannon" folder.

18. In C.S.'s review, he observed a series of images and videos in which at least three adult women are engaging in sex with at least two different minor victims. All three women are also seen in sexual images with the individual matching the description of **Tyrone Taylor**. C.S. also observed the individual matching the description of **Tyrone Taylor** sexually molesting at least two minor victims. C.S. estimates he recovered several thousand sexually explicit image and video files from the drive.

19. Based on the interview, and SA Thompson's observation of image file 20170109_180008.jpg, **Taylor's** hard drive and the two drives produced by 24 Hour Data were seized from 24 Hour Data and transported to the FBI Dallas Field Office at 1 Justice Way, Dallas, Texas.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

20. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed. Computers serve five functions in connection with child pornography: production, communication, distribution, storage and social networking.

21. Computers and cellular phones, along with the internet, permit adults to target and communicate with children in Internet chat rooms and through social networking sites. Frequently, they request photographs, including sexually explicit photographs, of those children. Any photographs received may be saved, forwarded, or downloaded to another computer, cellular phone, flash drive, or other electronic storage device. Unless deleted, these photographs may be maintained on a device for an indefinite period of time.

22. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. As with most digital technology, communications made from a computer are often saved or stored on that computer or on another electronic storage device, such as a flash drive. A forensic examiner often can recover evidence that shows whether a computer or other electronic device contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

23. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten.

24. For a number of reasons, the use of computers has become one of the preferred methods of trafficking in, trading, producing, and collecting child pornography and other obscene material. Because the distribution of child pornography is illegal, child pornography is not readily available through legitimate domestic businesses; in contrast, child pornography is widely available via computer from individuals who trade such materials on the Internet. Significantly, an individual can utilize a computer in the privacy of his/her own home or office to locate and interact with other individuals offering or seeking such materials. Moreover, he can do so without revealing his true identity. The use of computers thus provides individuals interested in child pornography or obscenity with a sense of privacy and secrecy. Computers also provide such individuals with a convenient method of storing, organizing, and accessing their collections and information concerning others who collect, trade, or distribute such materials.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

25. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics

common to individuals involved in the transportation, receipt and collection of child pornography:

a. Child pornography collectors usually start collecting child pornography by obtaining free images and videos of child pornography widely available on the internet on various locations and then escalate their activity by proactively distributing images they have collected, often for the purposes of trading images of child pornography with others, as a method of adding to their own collection of child pornography.

b. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

c. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media.

Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

d. Collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment.

These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

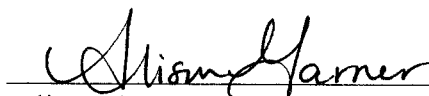
f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Given the voluminous number of images and videos discovered on **Taylor's** hard drive, **Taylor's** participation in sexual abuse of minors as well as the creation of visual depictions of those minors engaged in sexually explicit conduct, I believe Taylor is a collector of child pornography.

CONCLUSION

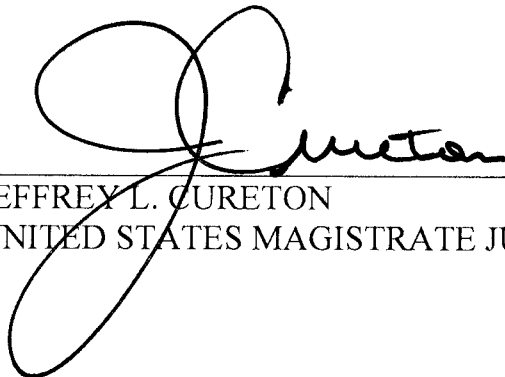
26. Based on the above information, there is probable cause to believe that the items described in Attachment B are presently located within the SUBJECT DEVICES,

as set forth in Attachment A, and that these items constitute evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252 and 2252A. Accordingly, I respectfully request that the Court authorize the search of the SUBJECT DEVICES and the seizure of the evidence and instrumentalities of the above violations of federal law and related contraband.



Alison Garner
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 7th day of August, 2019 at 1:55 p.m., in Fort Worth, Texas.



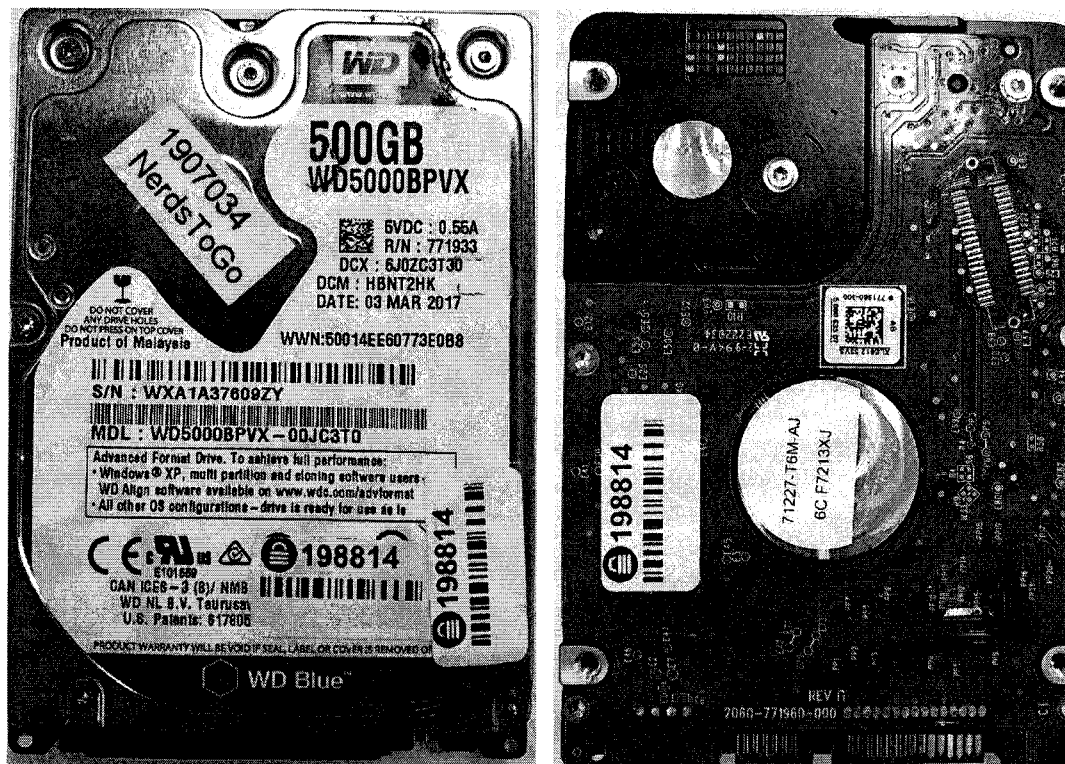
JEFFREY L. CURETON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF THE SUBJECT DEVICES TO BE SEARCHED

The following devices currently located at FBI Dallas Field Office at 1 Justice Way,
Dallas, Texas:

A Western Digital 500 GB hard drive, model WD5000BPVX bearing serial number WXA1A37609ZY. "Product of Malaysia" is printed on the drive label. This item is the original hard drive provided by Tyrone Taylor.



A Western Digital 1 TB hard drive, model WD10SDZW bearing serial number WXF1A288V7TR. This item contains a forensic acquisition of the Western Digital 500 GB hard drive, produced by 24 Hour Data.



A Toshiba 1 TB external hard drive, model DTB310 bearing serial number 77PXSIGLSTT1. This item contains a logical copy of files from the Western Digital 500 GB hard drive, produced by 24 Hour Data.



ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

The devices described in Attachment A and all records on the devices that relate to violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, 18 U.S.C. §§ 2251, 2252 and 2252A, including but not limited to:

1. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the production, possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256;
3. In any digital format and medium, all originals, computer files, copies, and negatives of child pornography and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, or child erotica;
4. Any and all digital diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer or by other means for the purpose of producing, distributing or receiving child pornography and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;
5. Any and all digital notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256;
6. Any and all digital notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the production, receipt, transmission, or possession of any child pornography as defined in 18 U.S.C. § 2256;

7. Any and all digital notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all digital notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

9. Any and all digital records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all digital records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

11. Any and all visual depictions of minors.

12. Any and all digital address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

13. Any and all digital diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Records of Internet Protocol addresses used; and

15. Records of internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.